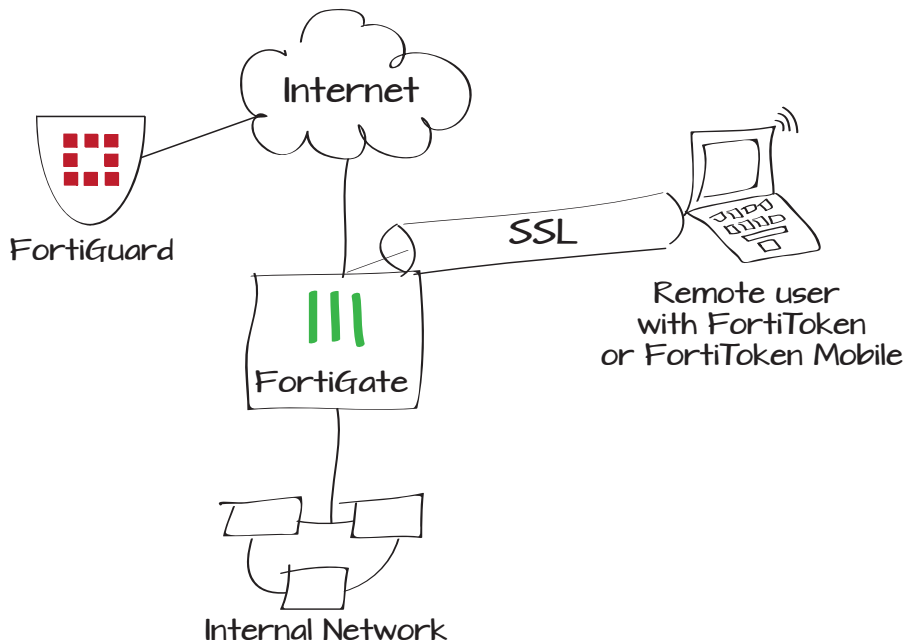


Using two-factor authentication with SSL VPN

An SSL VPN can use two-factor user authentication for enhanced security. In this example, a remote user uses FortiClient to connect to a private network behind a FortiGate unit. The FortiGate unit and FortiClient authenticate each other using a pre-shared key. The user is authenticated by User ID/password) plus a FortiToken token code.

1. Registering FortiToken with a FortiGate unit and FortiGuard
2. Adding two-factor authentication to the user's account
3. Defining an address for the internal network
4. Configuring the SSL VPN on the FortiGate unit.
5. Creating a security policy for SSL VPN users



Registering FortiToken with a FortiGate unit and FortiGuard

Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.

If you have several FortiTokens to add, you can list their serial numbers one per line in a text file and use the Import function.



FortiOS reports the serial number as invalid if you mistype it or if it is a duplicate.

Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.



If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.

Type

☒ Hard Token ☐ Mobile Token

Comments

0/255

Serial Number

Import

OK

Cancel

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	Available		0	

Adding two-factor authentication to the user's account

Go to **User & Device > User > User Definition** and open the user's account for editing.

Select **Enable Two-factor Authentication** and then select the FortiToken from the list. Select OK.

The screenshot shows the 'User Definition' configuration page for a user named 'tbrown'. The 'Password' section is active, showing a masked password and options to match users on LDAP, RADIUS, or TACACS+ servers. The 'Contact Info' section has 'Email Address' disabled and 'SMS' enabled, with a 'FortiGuard Messaging Service' selected and a phone number of '613-555-1200'. The 'Enable Two-factor Authentication' section is checked, with a token 'FTK2000BQL7PJW13' selected. A list of groups is shown, with 'full-time' selected. At the bottom are 'OK' and 'Cancel' buttons.

User Name: tbrown

☐ Disable

☒ Password: *****

☐ Match user on LDAP server: [Please Select]

☐ Match user on RADIUS server: [Please Select]

☐ Match user on TACACS+ server: [Please Select]

Contact Info

☐ Email Address

☒ SMS: ☒ FortiGuard Messaging Service ☐ Custom

Phone Number: 613-555-1200

☒ Enable Two-factor Authentication

Token: FTK2000BQL7PJW13

☒ Add this user to groups:

- ☐ FortiGate_Administrators
- ☐ SslvpnGroup
- ☐ WiFi_users
- ☒ full-time
- ☐ part-time

OK Cancel

Defining an address for the internal network

Go to **Firewall Objects > Address > Addresses** and select **Create New**.

The VPN configuration and the firewall policy require a defined address for the Internal network.

The screenshot shows the 'Address' configuration page for a new address named 'Local LAN'. The 'Category' is set to 'Address'. The 'Subnet / IP Range' is '192.168.1.0/255.255.255.0'. The 'Interface' is 'Any'. The 'Show in Address List' checkbox is checked. At the bottom are 'OK' and 'Cancel' buttons.

Category: ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name: Local LAN

Color: [Change]

Type: Subnet

Subnet / IP Range: 192.168.1.0/255.255.255.0

Interface: Any

Show in Address List: ☒

Comments: Write a comment... 0/255

OK Cancel





Creating a user group for SSL VPN users


Go to **User & Device > User > User Groups** and create a Firewall type user group, adding the users who will be permitted to use the SSL VPN.

Configuring an SSL VPN web portal

Go to **VPN > SSL > Config**.

The default encryption will work with typical browsers.

Name	<input type="text" value="full-time"/>
Type	<input checked="" type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest
Members	<div><div> tbrown ✕</div><div> jsmith ✕</div><div> blee ✕</div></div> <div></div>

IP Pools	<input type="text" value="SSLVPN_TUNNEL_ADDR1"/> ✕ 
Server Certificate	<input type="text" value="Self-Signed"/>
Require Client Certificate	<input type="checkbox"/>
Encryption Key Algorithm	<input type="radio"/> High - AES(128/256 bits) and 3DES <input checked="" type="radio"/> Default - RC4(128 bits) and higher <input type="radio"/> Low - RC4(64 bits), DES and higher
Idle Timeout	<input type="text" value="300"/> (seconds)
Login Port	<input type="text" value="10443"/>
<input type="checkbox"/> Allow Endpoint Registration (Tunnel Mode Only)	

▶ **Advanced** (DNS and WINS Servers)

Apply

Go to **VPN > SSL > Portal**.

Creating a security policy for SSL VPN users

Go to **Policy > Policy > Policy** and select **Create New**. Enter a policy to enable VPN users to authenticate and communicate with the local network.

Name:

web-access

Portal Message:

Welcome to SSL VPN Service

Theme:

Blue

Page Layout:

☐ Enable Tunnel Mode

☒ Enable Web Mode

Applications

☒ HTTP/HTTPS

☒ SSH

☒ CITRIX

☒ FTP

☒ TELNET

☒ RDP NATIVE

☒ RDP

☒ VNC

☒ Port Forward

☒ SMB/CIFS

☐ PING

☒ Include Session Info

☐ Include Connection Tool

☐ Include FortiClient Download

☒ Include Bookmarks

Create NewEdit SSL-VPN PortalDelete

Name	Type	Location	Description
No matching entries found			

☒ Prompt Mobile Users to Download FortiClient App

☒ Allow Multiple Concurrent Sessions For Each User

View Portal

Apply

Policy Type

☐ Firewall

☒ VPN

Policy Subtype

☐ IPsec

☒ SSL-VPN

Incoming Interface

wan1

Remote Address

all

Local Interface

port1

Local Protected Subnet

Local LAN

☐ SSL Client Certificate Restrictive

Cipher Strength

Any

Configure SSL-VPN Authentication Rules

Create NewEditDelete

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
<div>full-time</div>	ALL	always	-	full-access	<div></div>	<div>ACCEPT</div>
<div>ANY</div>	ALL	always	-		-	<div>DENY</div>

Tags

Applied tags

Add tag

Comments

Write a comment...

0/1023

OK

Cancel

Results

In a browser, enter the FortiGate IP address and port 10443. For example https://172.20.120.123:10443.

If you receive a warning about the certificate being unrecognized, allow the browser to continue access.

Enter the user name and password and then select **Login**. If the user account has two-factor authentication enabled, the **FortiToken Code** field is added. Obtain the code from the FortiToken device or FortiToken Mobile app and enter it. Select **Login** again.

You are connected to the SSL VPN portal.

The **VPN > Monitor > SSL-VPN Monitor** page shows the connected SSL VPN client.

Please Login

Name:

tbrown

Password:

.....

FortiToken Code:

.....

Login

Welcome to SSL VPN Service

?

Help

Logout

Session Information

Time Logged In:

tbrown (0 hour(s), 0 minute(s), 41 second(s))

HTTP Inbound/Outbound Traffic:

0 bytes / 0 bytes

HTTPS Inbound/Outbound Traffic:

0 bytes / 0 bytes

Remote Desktop

[Windows server](#)

[telbar PC](#)

Add

Edit

Tunnel Mode

Connect

Disconnect

Refresh

Link status:

Bytes sent:

Bytes received:

Collecting information...

Connection Tool

Type:

HTTP/HTTPS

Host:

Go

<input type="checkbox"/>	No.	User	Source IP	Begin Time	Description
<input type="checkbox"/>	1	tbrown	172.20.120.52	Thu Sep 12 10:04:32 2013	
<input type="checkbox"/>			Subsession		Tunnel IP:10.212.134.200